Magic

Middleware for collaborative Applications and Global virtual Communities

CAREN

Magic Project: Introduction and AAI

Almaz Bakenov

director@it.kg

National Information Technology Center

CAREN Regional Networking Conference 2017

Bishkek, Kyrgyz Republic

25-26 April 2017

Magic Project

- European Union’s Horizon 2020 Programme
- **Objectives:**
  - To enable mobility and seamless access to services by:
    - promoting the establishment of identity federations connected to eduGAIN,
    - creating awareness of privacy and security issues, and
    - increasing uptake of eduroam
  - To enable the provision of collaboration tools and services among NRENs based on NREN-run applications made available via a worldwide application market.

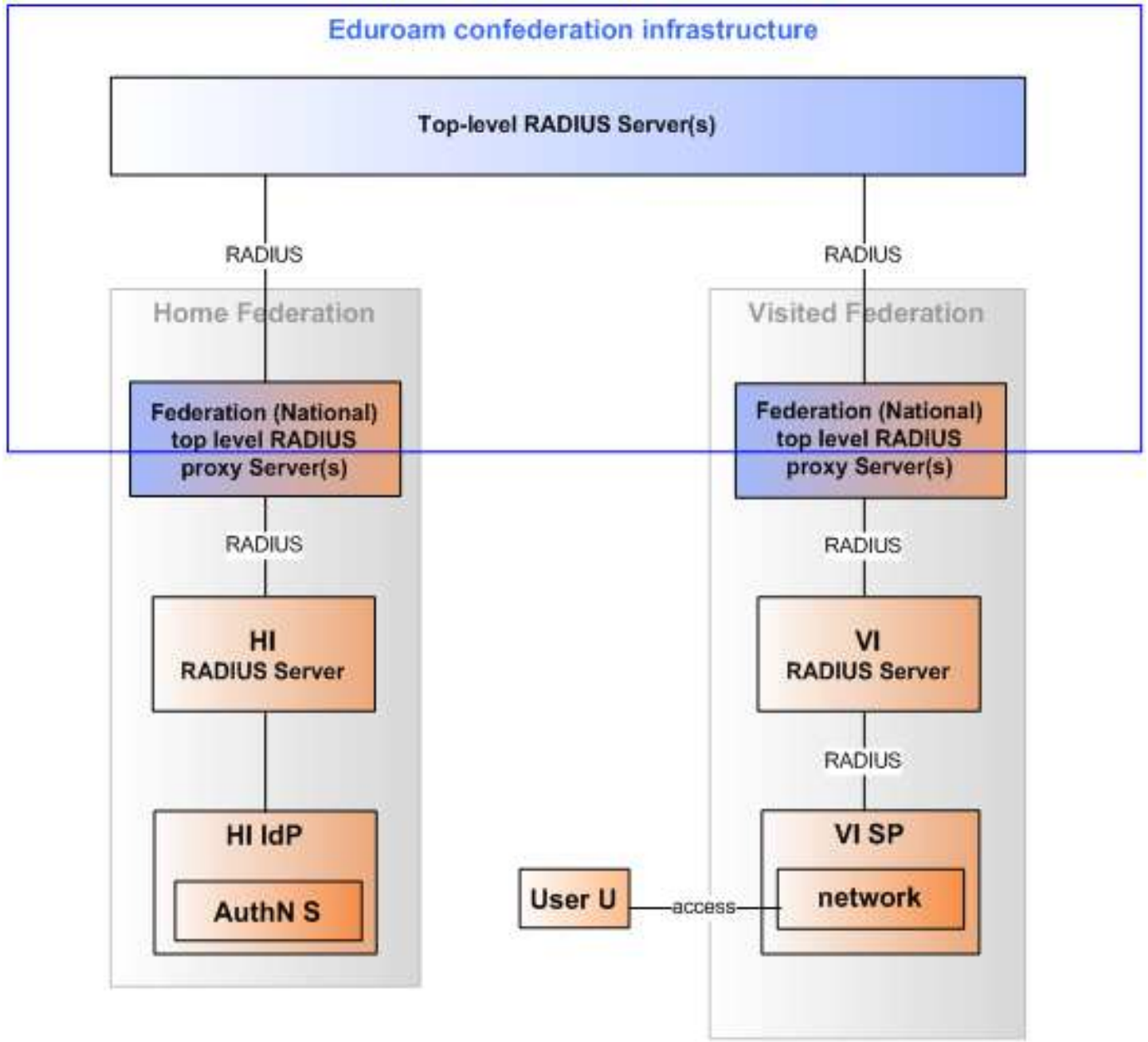
Magic Project partners

Grant Partners:

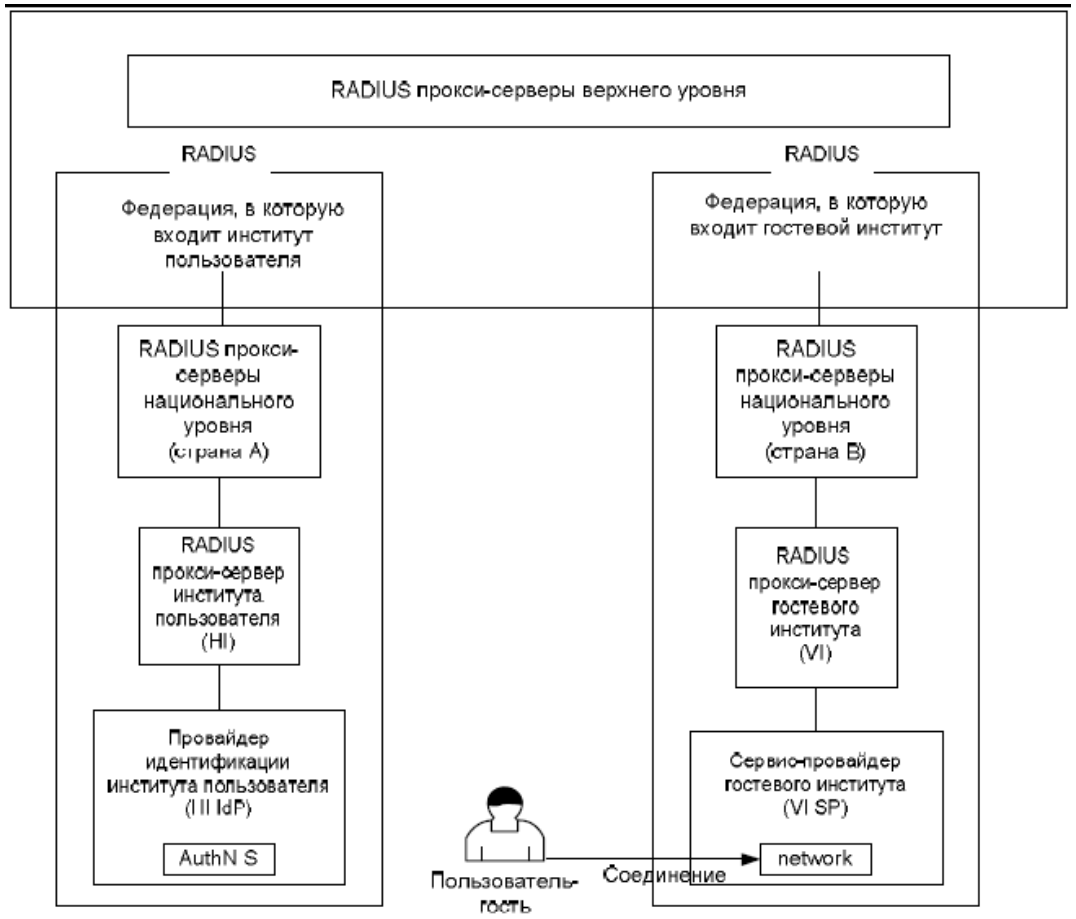
- RedCLARA (Latin America) - coordinator
- GÉANT (Europe)
- RENATA (Colombia)
- RNP (Brazil)
- SURFnet (Netherlands)
- REUNA (Chile)
- CEDIA (Ecuador)
- CUDI (Mexico)
- RENATER (France)
- GRNET (Greece)
- CESNET (Czech Republic)
- CKLN (Caribbean)
- UbuntuNet Alliance (S&E Africa)
- WACREN (W&C Africa)
- ASREN (Arab States)
- TEIN*CC (Asia-Pacific)
- CAREN NOC – NITC (Central Asia)
- NIIFI (Hungary)
- CSIR (South Africa)

- MoU Partners
- APAN (Asia-Pacific)
- AARNET (Australia)
- InnovaRed (Argentina)
- EthERNet (Ethiopia)
- RENAM (Moldova)

Eduroam


Eduroam confederation infrastructure
Top-level RADIUS Server(s)
RADIUS
RADIUS
Home Federation
Visited Federation
Federation (National) top level RADIUS proxy Server(s)
Federation (National) top level RADIUS proxy Server(s)
RADIUS
RADIUS
HI RADIUS Server
VI RADIUS Server
RADIUS
RADIUS
HI IdP
AuthN S
VI SP
network
User U
access

http://cyberleninka.ru/article/n/udostoveryayuschie-federatsii-nauchno-obrazovatelnyh-setey.pdf



HI – институт пользователя, VI – гостевой институт, IdP – провайдер идентификации, SP – институтский провайдер доступа к сети

Рис. 1. Конфедеративная инфраструктура eduroam

http://cyberleninka.ru/article/n/udostoveryayuschie-federatsii-nauchno-obrazovatelnyh-setey.pdf

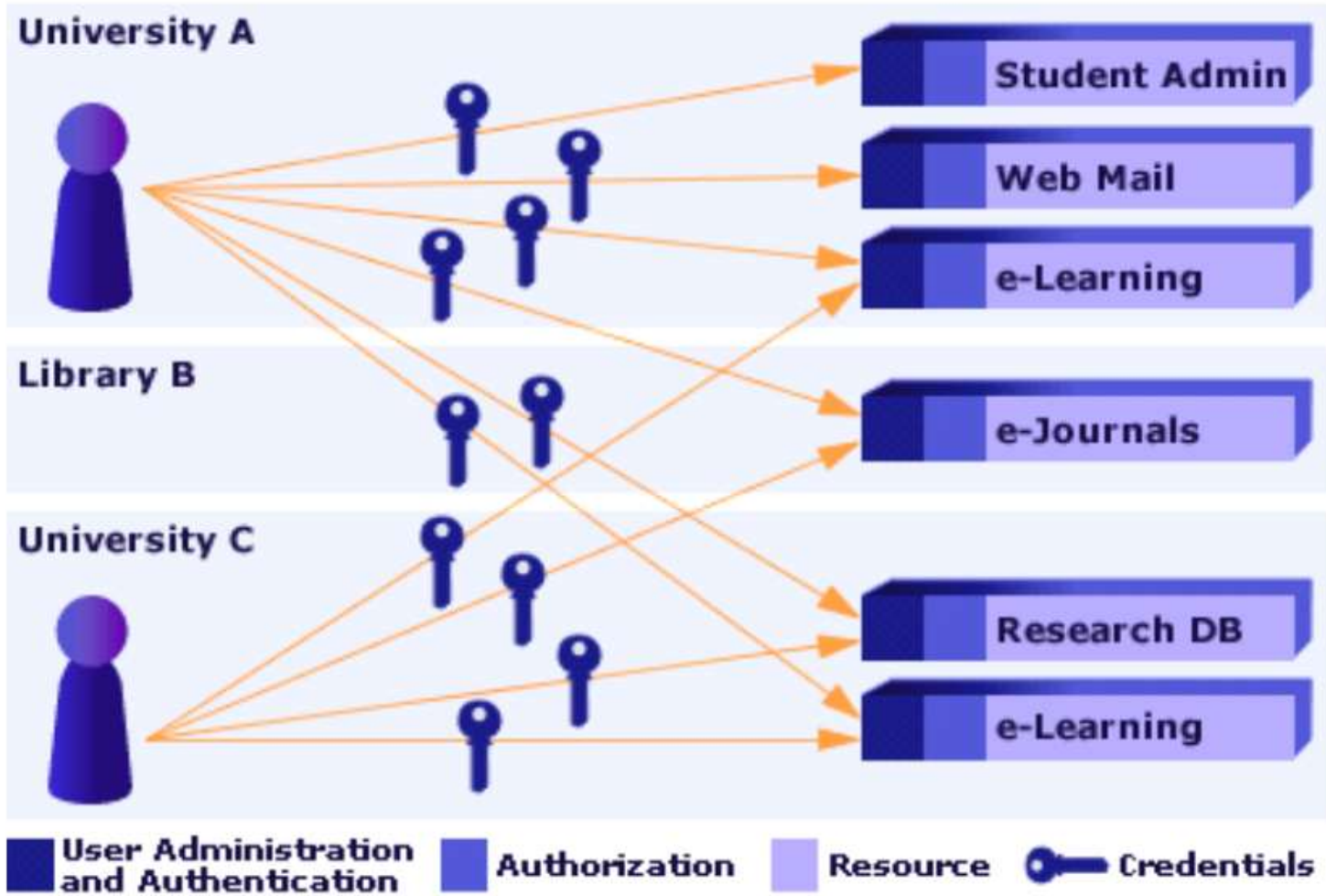
- Identity federation

- Удостоверяющая федерация – объединение институтов в научно-образовательных сетях, предоставляющих так называемую технологию «единого входа» (Single Sign On) для доступа к своим ресурсам.

Federated authentication and authorization infrastructure

Magic
Middleware for collaborative Applications and Global virtual Communities

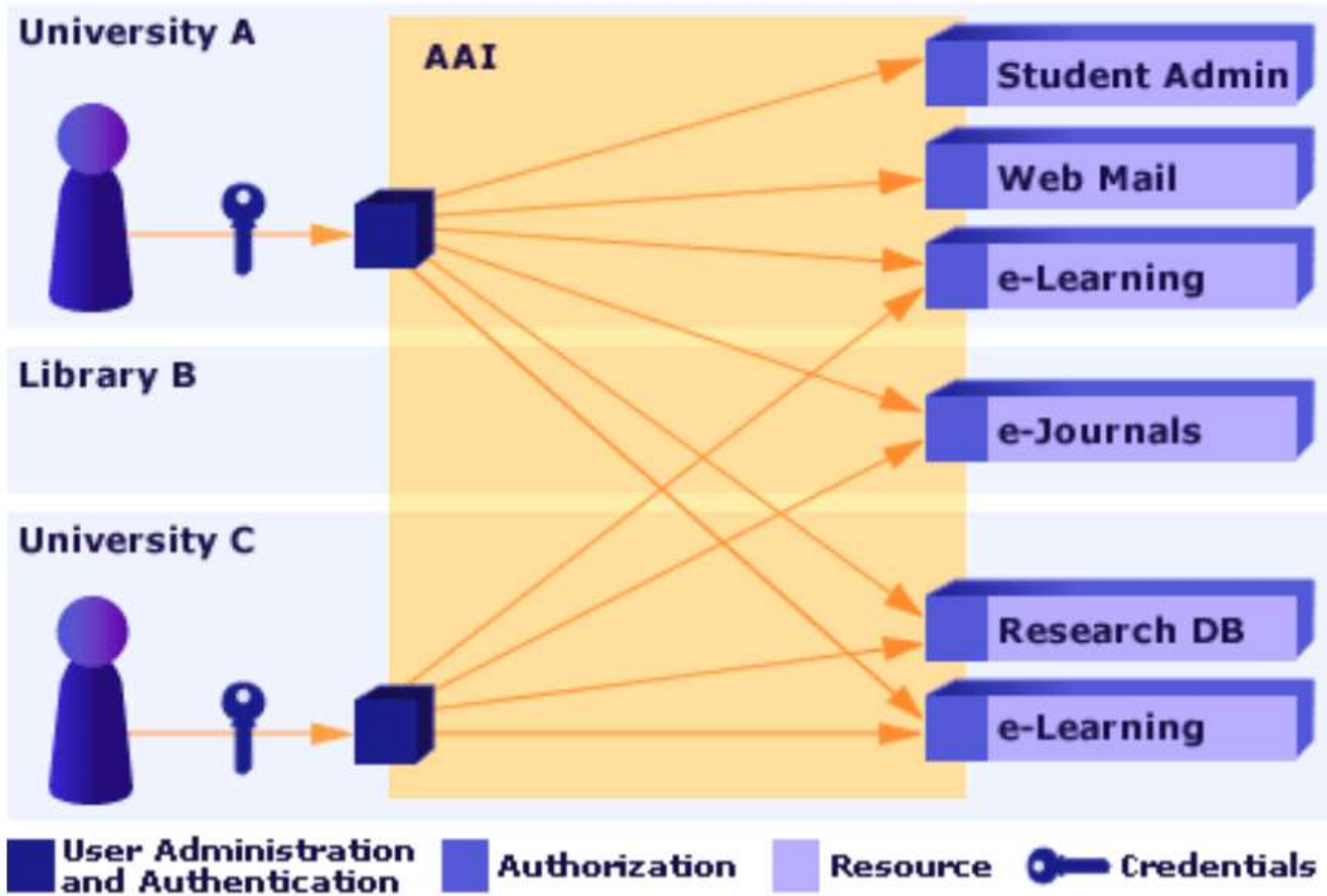
Fonte: SWITCH AAI-Federation

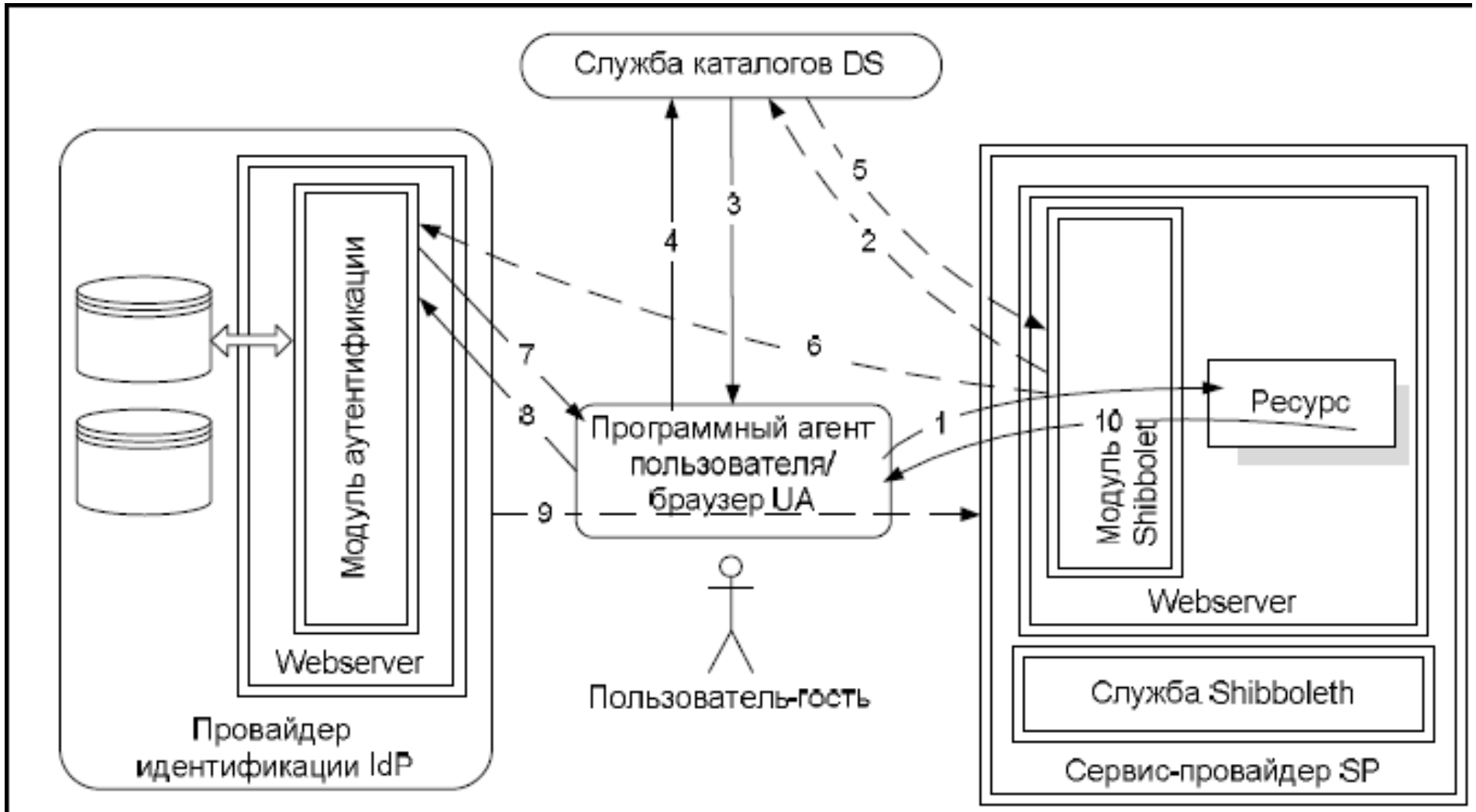


Federated authentication and authorization infrastructure

Magic
Middleware for collaborative Applications and Global virtual Communities

Fonte: SWITCH AAI-Federation





1 – UA требует у SP доступ к ресурсу; 2 – SP перенаправляет UA к DS для выбора IdP; 3, 4 – Выбор IdP; 5 – перенаправление к SP с выбранным IdP в качестве параметра; 6 – SP направляет SAML-запрос на аутентификацию IdP; 7, 8 – аутентификация у IdP; 9 – IdP направляет SP SAML-ответ с атрибутами пользователя; 10 – UA получает доступ к Ресурсу.

Рис. 2. Процедура авторизации в архитектуре Shibboleth

http://cursos.redclara.net/course/view.php?id=51

1. In this chapter, the basic concepts of AAI are covered, helping students to understand all pieces of an identity federation.
   - Introduction and AAI Concepts PDF document

2. In the second chapter of this course, it is approached how to implement an Identity Provider (IdP)
   - Identity Provider Concepts and Implementation PDF document

3. After covering the basic aspects af AAI and show how to raise an IdP, now it is necessary to explain the purpose of a Federation, explaining what is a Service Provider (SP), how to implement and what is an Interfederation, like eduGAIN.
   - Service Provider Concepts, Implementation and Interfederations PDF document

4. The foundation of a Identity Federation is the trust between members, because of that, one of the most important part of this course covers the governance and the best practices.
   - Identity Federation Governance and Best Practices

Federated authentication and authorization infrastructure

- **Examples of inner services**:
  - Project registration, registration of students, record notes, document sharing etc.
- **Examples of outter services :**
  - Access to digital libraries, resource sharing (CPU cycles, storage space), distance learning etc.
- A federation offers to institutions the authentication and authorization infrastructure necessary to interconnect people and share resources, information and services

Evolution of Identity Management

				
Primordial Soup	Stone Age	Bronze Age	Iron Age	Diamond Age
• Nothing yet!	• Application holds all info	• Centralised credential e.g. LDAP • Identity in app	• Central credentials and Identity • App only has specific user data	• Federated Identity • Share information outside one domain

Ann Harding, SWITCH
Cambridge
July 2014